Bellcore
Bell Communications Research

EX PARTE OR LATE FILED

Michael J. Knapp
Director- Federal Relations

WAS-600
2101 L Street NW
Washington, DC 20037-1585
202-776-5454
Fax 202-776-5424
Email mknapp@notes.cc.bellcore.com

March 5, 1997

Mr. William F. Caton
Acting Secretary
Federal Communications Commission
1919 M Street, N.W., Room 222
Washington, DC 20554

Re: CC DOCKET NO. 95-116, Telephone Number Portability

Dear Mr. Caton:

On February 19, 1997, SBC Communications, Inc. filed with the Commission a copy of a Bellcore study regarding the risk of network failure in the Houston MSA if current plans for implementing local number portability (LNP) are implemented. That filing led to a response by letter dated February 26, 1997 from Mr. Salemme, AT&T's Vice-President - Government Affairs, in which he characterizes the Bellcore study as flawed.

Bellcore continues to believe that its analysis of the risks in the current LNP deployment plan is correct. In an attachment to this letter we respond in detail to specific points in Mr. Salemme's letter. In addition, we wish to highlight four points.

First, the letter repeatedly states or implies that the types of failures considered in the Bellcore analysis are too improbable to be of concern. This is incorrect. In fact, AT&T's own network suffered just such an "improbable" fate on January 15, 1990 when obscure and trivial errors resulted in a prolonged and agonizing succession of switch failures which cascaded back and forth across the nation. Virtually all of AT&T's switches were affected. A front page article from the January 17, 1990 New York Times said:

> "The American Telephone and Telegraph Company said yesterday that it had traced the huge disruption in long distance calling to a single computer program that malfunctioned and caused a chain reaction in the network... The faulty program, a new version of switching software, sent a swarm of overload signals... A.T.&T. has still not explained why the system failed to compensate for the failure of a single component, but the failure is seen as troubling evidence of how vulnerable technology-based systems are to even slight disruptions."

Similar experiences occurred in 1991 in networks of two Local Exchange Companies, Bell Atlantic and Pacific Bell, when a combination of events and errors caused Signal Transfer Points to fail. In the outage that isolated Washington DC, a pair of STPs failed (and then the other mated pair also failed). Disastrous

outages have also occurred in Singapore and elsewhere. In Singapore, a faulty patch brought over 90% of the local switches down simultaneously; the problem cascaded across the entire network.

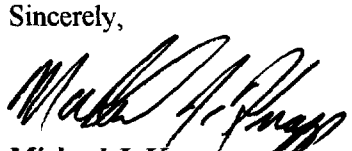
There has not been a failure of a mated pair of SCPs, at least as "failure" is technically defined – probably because of extreme vigilance and light loads. However, there have been two events that can only be described as "near death experiences." In one case, one SCP failed and the SCP's mate was so severely stressed that it could not be accessed to check its condition. In another case, the 3 processors in one SCP failed and 2 out of 3 processors in the mate failed. Thus, even though a complete failure event did not occur, these circumstances indicate that there is certainly a reasonable probability of such an event occurring. In the United States, such partial and complete failures have been relatively rare because we anticipate their occurrence, and, as an industry, we go to great efforts to reduce their likelihood and their impact.

Second, more generally, it is improper to cite the limited number of failures as some form of proof that there is limited risk of failure. What it proves is that we have, as an industry, been diligent in anticipating failures, guarding against them, and adopting designs and procedures that minimize their effects when they occur.

Third, we were extremely conservative in our estimates of the chances of various types of failures. For example, we did not include potential effects of any security intrusions or sabotage. Hank Kluepfel at the most recent Network Reliability Steering Committee meeting on Feb. 27 stated, "Security intrusions are known to occur when new software is put in the network." We also did not factor in the effects of human errors, Operations Support Systems, message looping problems, or default traffic on the reliability of the network. Each of these make the network more vulnerable when new software and systems are deployed, and their combined effect could potentially dwarf any failure estimates that we provided.

And fourth, the risks that we discuss are real, and can and should be avoided. A more prudent schedule will enable the industry to provide enough testing and soaking of the systems involved. Adequate industry interoperability testing for LNP will be essential to minimize risks of failure. As we noted in the analysis, with LRN (without QoR) virtually all interoffice calls will be affected by SCP failures, while with LRN augmented with QoR only a tiny fraction of calls will be affected by such failures. To implement LNP without sacrificing telecommunications reliability – a level of reliability that subscribers have experienced and expected for many years – requires an implementation that thoroughly tests each step and puts a minimal set of customers at risk if a failure does occur. LRN augmented by QoR as an initial implementation of LNP meets this need, and should not be foreclosed, either as an interim implementation (pending testing, soaking and integrating LNP implementations) or as a final one.

Sincerely,



Michael J. Knapp

ATTACHMENT

This attachment provides Bellcore responses to some of the specifics in the letter from Mr. R. Gerald Salemme, AT&T's Vice-President - Government Affairs, to the Acting Secretary, Mr. William F. Caton, dated February 26, 1997.

1) PAGE 2. *"The study describes a highly improbable scenario in which all LNP SCPs in the Houston MSA fail ... simultaneously ..., SBC was forced to stretch statistical credibility ... the study assumes that there is a 90% probability that if the first mated SCP pair fails, the second mated SCP pair will also fail at the same time."*

Bellcore Reply: The above excerpts and related material in the letter may be summarized by saying that AT&T's view is "This just can't happen, the probabilities are too small". However, similar events have occurred, in AT&T's network and networks of other service providers (see main letter).

We believe that the parameters are of the correct magnitude. Moreover, the parameters we employed correspond closely with values that have been used by Bellcore and various Local Exchange Carriers over many years in their efforts to assess and improve the reliability of their networks. In this process, these values have been reviewed by countless engineers and other professionals and found to be reasonable and suitable for their applications.

2) PAGE 2. *"If the logic of the SBC study is to be credited, then the probability of 10 mated SCP pairs failing simultaneously is 3.87 times higher than a single pair failing simultaneously. This result is inherently illogical."*

Bellcore Reply: This assertion is not true and Bellcore's past analyses of multiple system failures validates the Bellcore model. A common theme in significant failures that we considered (AT&T switches in 1990, Bell Atlantic and Pacific Bell STPs in 1991, and a near-total failure of a mated pair of SCPs) is that a trigger event of somewhat random nature often starts a cascade of subsequent failures. The occurrence of such a trigger is reasonably modeled as being proportional to the number of components (STPs in this case). Doubling the number of components doubles the risk, contrary to Mr. R. Gerald Salemme's claims.

As a specific example, the near-miss SCP failure was initiated because of ill considered but intentional asymmetries in the use of the two SCPs in a pair. Combined with other errors and events, a near failure occurred. Because each SCP in the pair was unique with respect to this class of failures, each had a separate, stochastically independent exposure to such a fault. Thus, their failure rate for this class of failures was for all practical purposes twice that of a single SCP.

3) Page 3 *"The third fundamentally incorrect assumption the study employs is that the use of switch-based software fault factors increases the likelihood that components other than the switch will fail. There are two obvious flaws in this logic. First the study assumes that a factor*

derived from the total number of software faults, many of which produce only minor errors, is an accurate predictor of software faults that will produce a catastrophic network failure."

Bellcore Reply: Mr. Salemme also objected that the fault data that we used might include minor faults and therefore would not be a good predictor of outages. In fact, we used every piece of data that was available and they all resulted in the same conclusion. We observed similar results from graphs of critical faults and major faults. For one of the switches, the number of minor faults is less than 1/8th of all faults so that including minor faults made no difference. In addition, we utilized outage data for one vendor's switches and found the same pattern.

Also Mr. Salemme's position that we need not worry about "minor" software errors is incorrect. There is no such thing as a benign or "minor" error when predicting the risk of system failure. Any error in any part of the software has the potential to fail a system. Examples of this include:

- The recent failure of the newest Ariane rocket and the destruction of its three satellite payload was caused by a "minor" error in a system that was performing no needed function at the time. Unfortunately, the software was not designed to isolate the impact of that particular error (which was truly trivial) and the mission was terminated as a result.
- Any frequent user of a personal computer has experienced the disappointment of a total system failure as the PC screen "locks" for no apparent reason while performing some routine task. Usually, the PC must be rebooted, disrupting any programs that may still be working in the background and often causing data to be lost.

4) PAGE 3. *"the SBC study applies its flawed switch-based software factors to predict a purported increase in the probabilities of a network failure in other signaling system components (i.e., STPs and SCPs). Bellcore concedes it has no data on the software failure history for common channel signaling ("CCS"), Advanced Intelligent Network ("AIN") or 800-databases to support its suppositions".*

Bellcore Reply: Bellcore assumed that complex software in STPs and SCPs are consistent with the general reliability trends for switch software. This is a conservative assumption. Actually with the involvement of new vendors of software, we can anticipate even greater multipliers when testing and soaking are cut short, because of the potential for initial incompatibilities. Virtually every software reliability model assumes growth. Every system that we have seen with software reliability data follows a similar pattern.

In contrast, Mr. Salemme would assume a zero probability of failure for subsets of software products for which failure data are limited, or for which our efforts to prevent failures over the past few years have been successful. Bellcore believes that its assumptions more appropriately model the risks than an assumption that there is no risk.